# ENHANCED DYNAMIC SECURITY ASSESSMENT FOR POWER SYSTEM UNDER NORMAL AND FAKE TRIPPING CONTINGENCIES.

QUSAY A. SALIH

A thesis submitted in
fulfillment of the requirement for the award of the
Doctor of Philosophy in Electrical Engineering

Faculty of Electrical and Electronic Engineering
Universiti Tun Hussein Onn Malaysia

AUGUST 2019

I dedicated this thesis to my family and friends for their valuable support and encouragement during my research study and a special dedication to my uncle's late family, who lost their lives during the attack in Mosul.

## ACKNOWLEDGEMENT

First of all, gratefulness of thanks to our Creator “ALLAH” who enabled us to complete this thesis.

Special thanks go to my supervisor Dr. Mohd Aifaa bin Mohd Ariff, for having this opportunity to work under his supervision and for sharing his great knowledge and experience with me.

## ABSTRACT

Recently, power system networks have become more dependent on new technologies especially in using a communication network to enhance the overall performance of system operation. The communication network facilities are applied to send and receive data and commands through the wide-area power network. However, this dependency has opened a new threat of fake tripping contingency towards the power system operation. This challenge has motivated this study to ensure that all analytical tools applied during power system operation are not affected under fake tripping contingency, especially on dynamic security assessment (DSA) classifier. To address this challenge, this study aims to invistigate the impact of fake tripping contingency on the power system security via DSA classifier, then develop a novel hybrid approach for DSA classifier based on advanced feature selection technique for decision tree (DT) classifier and finally evaluate the performance of DSA classifier under normal and fake tripping contingencies, in terms of accuracy and computational time. The hybrid logistic model tree (hybrid LMT) approach proposed in this study combines the symmetrical uncertainties (SU) algorithm and the logistic model tree (LMT) algorithm. The training dataset is built by applying all possible contingencies during normal and fake tripping scenarios to the test system models. The effectiveness of the proposed approach is demonstrated on modified IEEE 9-, 14-, and 30-bus test system models due to the limitations in the simulator program. The results indicate that the hybrid LMT accurately assesses the dynamic security status of the system under normal and fake tripping contingencies with short time frame. The results show that the proposed method has 98.4126%, 98.3606%, and 99.537% accuracy and requires 22.22%, 23.529 % and 25.27% less computational time as compared to the conventional LMT algorithm in assessing the dynamic security status of the IEEE 3-machıne 9-bus, the IEEE 5-machıne 14-bus, and the IEEE 6-machıne 30-bus test system models, respectively. In summary, the results obtained in this study offer accurate and high-speed information for the dynamic

security state, which makes DSA classifier able to provide vital information for protection and control applications to keep the power system in a secure and reliable state.

**ABSTRAK**

Terkini, rangkaian sistem kuasa semakin bergantung kepada teknologi baru, terutamanya kepada penggunaan rangkaian komunikasi untuk meningkatkan prestasi keseluruhan operasi sistem tersebut. Kemudahan rangkaian komunikasi digunakan untuk menghantar dan menerima data serta arahan melalui rangkuman meluas rangkaian kuasa. Namun, pergantungan ini telah mencipta suatu ancaman baharu iaitu kontingensi gangguan palsu terhadap operasi sistem kuasa. Cabaran ini telah mendorong kajian ini untuk memastikan bahawa semua peralatan analisis yang digunakan sepanjang operasi sistem kuasa tidak akan terkesan akibat kontingensi gangguan palsu, terutamanya terhadap pengkelas penilaian keselamatan dinamik (DSA). Untuk menangani cabaran ini, kajian ini berusaha untuk mengkaji kesan kontingensi gangguan palsu terhadap keselamatan sistem kuasa melalui pengkelas DSA. Kemudian, kajian ini akan membangunkan suatu pendekatan hibrid baharu untuk pengkelas DSA berasaskan teknik pemilihan ciri lanjutan untuk pengkelas pokok keputusan (DT), dan akhir sekali, menilai prestasi pengkelas DSA di bawah kontingensi normal dan kontingensi gangguan palsu, dari segi ketepatan dan masa pengiraan. Pendekatan pokok model logistik hibrid (LMT) yang dicadangkan di dalam kajian ini menggabungkan algoritma ketakpastian simetri (SU) dan algoritma pokok model logistik (LMT). Set data latihan dibina dengan menggunakan semua kemungkinan kontingensi semasa senario serangan normal dan serangan gangguan palsu ke atas model-model sistem ujian. Keberkesanan pendekatan yang dicadangkan ini dibuktikan melalui model-model sistem ujian terubahsuai IEEE 9-, 14-, dan 30-bas akibat kekangan di dalam program simulator. Keputusan menunjukkan bahawa LMT hibrid ini berjaya menilai status keselamatan dinamik sistem secara tepat di bawah kontingensi normal dan kontingensi gangguan palsu dalam tempoh yang singkat. Keputusan menunjukkan bahawa kaedah yang dicadangkan mempunyai 98.4126%, 98.3606%, dan 99.537% ketepatan dan memerlukan 22.22%, 23.529%, dan 25.27% kurang masa pengiraan berbanding dengan algoritma LMT yang

konvensional dalam menilai status keselamatan dinamik model-model sistem ujian masing-masing IEEE 3-mesin 9-bas, IEEE 5-mesin 14-bas, dan IEEE 6-mesin 30-bas. Kesimpulannya, keputusan yang diperoleh di dalam kajian ini menawarkan maklumat yang tepat dan berkelajuan tinggi untuk keadaan keselamatan dinamik yang menjadikan pengkelas DSA berupaya memberikan maklumat penting untuk perlindungan dan aplikasi kawalan demi memastikan sistem kuasa berada di dalam keadaan yang selamat dan boleh dipercayai.

# CONTENTS

# LIST OF TABLES

## LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | | |
|---|---|---|
| DSA | - | Dynamic Security Assessment |
| DT | - | Decision Tree |
| EPRI | | Electric Power Research Institute |
| IEEE | - | Institute of Electrical and Electronics Engineers |
| LMT | - | Logistic Model Tree |
| NERC | - | North American Electric Reliability Council |
| PJM | | Interconnection power system in the United States of America |
| PMU | - | Phasor Measurement Units |
| Rated kV | - | Machine-rated terminal voltage in kV; base kV for impedances |
| Rated MVA | - | Machine-rated MVA; base MVA for impedances |
| SU | - | symmetrical uncertainty |
| $D$ | - | Machine load damping coefficient |
| $E_1$ | - | Field voltage value,1 in p.u. |
| $E_2$ | - | Field voltage value,2 in p.u. |
| $F$ | - | Shaft output ahead of reheater in p.u. |
| $H$ (s) | - | Inertia constant in s |
| $K_a$ | - | Regulator gain (continuous acting regulator) in p.u. |
| $K_e$ | - | Exciter self-excitation at full load field voltage in p.u. |
| $K_f$ | - | Regulator stabilizer circuit gain in p.u. |
| $P_{max}$ | - | Maximum turbine output in p.u. |
| $R$ | - | Turbine steady-state regulation setting or droop in p.u. |
| $S(1.0)$ | - | Machine saturation at 1.0 p.u. voltage in p.u. |
| $S(1.2)$ | - | Machine saturation at 1.2 p.u. voltage in p.u. |
| $S_{E(E1)}$ | - | Saturation factor at E1 |
| $S_{E(E2)}$ | - | Saturation factor at E2 |
| $T''_{d0}$ | - | d axis subtransient open circuit time constant in s |
| $T''_{q0}$ | - | q axis subtransient open circuit time constant in s |

| | | |
|---|---|---|
| $T'_{d0}$ | - | d axis transient open circuit time constant in s |
| $T'_{q0}$ | - | q axis transient open circuit time constant in s |
| $T_1$ | - | Control time constant (governor delay) in second |
| $T_2$ | - | Hydro reset time constant in second |
| $T_3$ | - | Servo time constant in second |
| $T_4$ | - | Steam valve bowl time constant in second |
| $T_5$ | - | Steam reheat time constant in second |
| $T_a$ | - | Regulator time constant in second |
| $T_e$ | - | Exciter time constant in second |
| $T_f$ | - | Regulator stabilizing circuit time constant in second |
| $T_r$ | - | Regulator input filter time constant in second |
| $V_{Rmax}$ | - | Maximum regulator output, starting at full load field voltage in p.u. |
| $V_{Rmin}$ | - | Minimum regulator output, starting at full load field voltage in p.u. |
| $r_a$ | - | Armature resistance in p.u. |
| $x''_d$ | - | Unsaturated *d* axis subtransient reactance in p.u. |
| $x''_q$ | - | Unsaturated *q* axis subtransient reactance in p.u. |
| $x'_d$ | - | Unsaturated *d* axis transient reactance in p.u. |
| $x'_q$ | - | Unsaturated *q* axis transient reactance in p.u. |
| $x_d$ | - | Unsaturated *d* axis synchronous reactance in p.u. |
| $x_l \; or \; x_p$ | - | Leakage or Potier reactance in p.u. |
| $x_q$ | - | Unsaturated *q* axis synchronous reactance in p.u. |

## LIST OF APPENDICES

# CHAPTER 1

# INTRODUCTION

## 1.1 Introduction

The electric power system network is the backbone of energy in any country. It is responsible for transmitting power to the customers from the generation side through a wide and complex network that includes a huge number of devices and equipment. In general, this network contains two crucial layers. The first layer is responsible for facilitating electricity flows from the utility to the customer. This layer is divided into three main sections, namely, generation, transmission, and distribution. The second layer is responsible for facilitating communication for power system operation. This layer sends control commands and receives information from the power carry layer to the control center. Figure 1.1 shows the general layers in a power grid infrastructure.

The communication network layer includes different media, such as telephone lines, microwaves, satellites, and fiber optics. The communication network offers many advantages for the control center operation, while simultaneously reducing the operation cost for the power system. Therefore, electrical utilities have made various efforts to develop this vital network and its operation. However, a communication network is prone to failures due to different reasons, which include human error, malfunctioning of equipment, and limitations of the communication architecture and cyber-attack. Based on a report by the North American Electric Reliability Council (NERC), failures in communication and information system is the root cause of 32% of power outages [2]. For example, one of the reasons for the North America blackout in 2003 was a computer system's failure that send an

unwanted alarm signal to the control center [3]. Therefore, communication failures have a significant impact on power system operation.

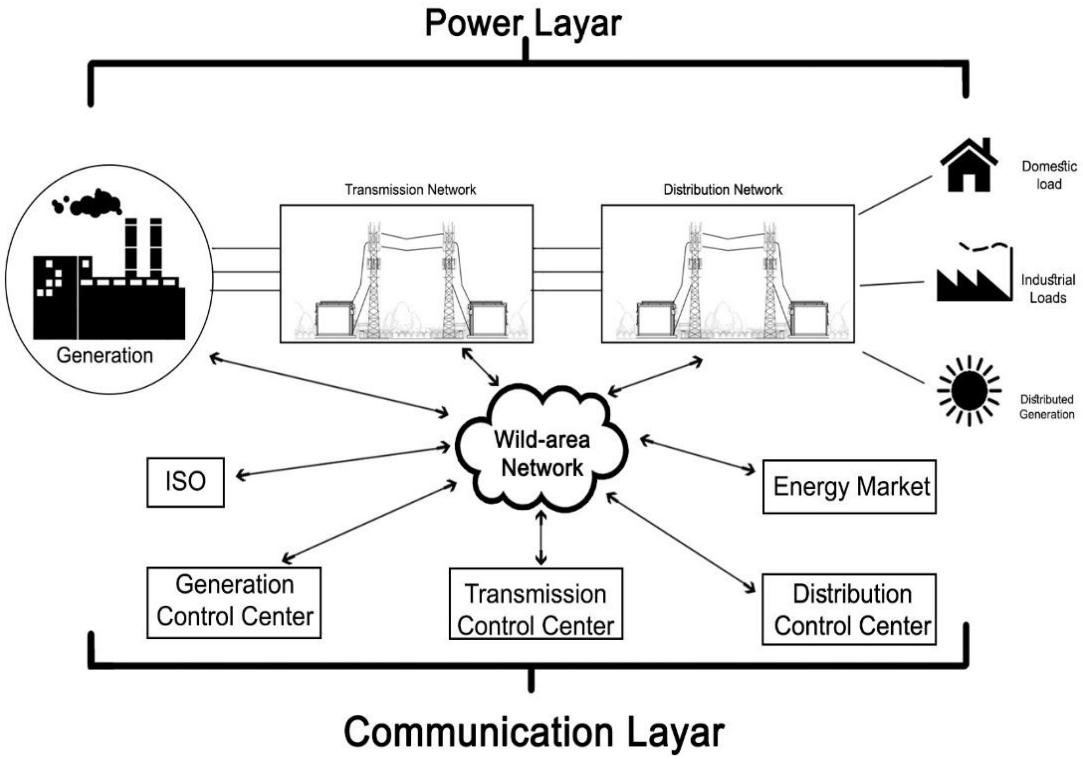


Figure 1.1: Power grid infrastructure [1]

The high integration of communication technology into the power grid which uses a weak secured communication protocol in sending and receiving data and commands through wide power network makes it more vulnerable to the new threat to the power grid that is fake tripping. Where fake tripping could trigger the circuit breaker (open/close) and cause a fake tripping contingency on the power system. One off fake tripping is cyber-attack [4]. Based on Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector report, cyber-attack is “an attempt to infiltrate information technology systems, computer networks, or individual computers with a malicious intent to steal information, cause damage, or destroy specific targets within the system” [5]. The impact of a cyber-attack in the power system could be devastating for electric companies and users. This is for the ability of the attacker to make a direct impact on the power transmission operation. The cyber-attack could access the communication network via various technical channels where an attacker could exploit the weaknesses in protection procedures or the weaknesses in data encryption sent over the wide network.

In general, a cyber-attack in the power system can be classified into two types: individual and non-individual. The individual attack is simpler between these two attacks where the target of this one is to change the consumed power by the users by hacking the smart electric meter to reduce the cost of electricity bills [6]. While, the non-individual attack is the dangerous attack aiming to cut off the electrical service by trying to access the generators, control or protection devices or control for the drop load. This kind of attack is usually based on the ideology adopted by the attackers, such as terrorism or political conflicts. As an example, the Ukraine blackout in December 2015 was due to a confirmed cyber-attack [7].

It is worth noting that the main concern with cyber-attacks is that: the attacker will always try to cause major harm to the power grid by using different ways and techniques that could give them the authorizing access to the grid, without leaving any "fingerprints" if possible (e.g., there are various ways and channels for these attackers to gain access to the network). Meanwhile, the main target of the control center is to keep the power system secure by using traditional techniques and training. Thus, each one has a different perspective and training. Therefore, it is very challenging for the network operator to consider or estimate all possible attack scenarios in a very wide and complex system. There is no guarantee that the power grid can be 100% secured from cyber-attacks since the game between an attacker and a control center is a dynamic game. To develop a better defense strategy for the power grid, the control center should follow an optimization approach for example using Game Theory [8] to reach a strategy where the system has no incentive to change its strategy (Nash Equilibrium), taking into account normal and cyber-attack contingencies as cost functions in the optimization design. Definitely, this kind of defense strategy could not prevent cyber-attacker, but it is able to help system operator to mitigate the server of cyber-attack contingency and prevent the blackout.

In order to keep the power system in a reliable and secure state, control centers should evaluate the security of the system following contingencies via a dynamic security assessment (DSA) tool. The DSA is an essential tool for monitoring and of assessing the state of security of the power system’s behaviors (meaning secure or insecure) after a contingency has occurred. Therefore, studying the impact of contingency that is caused by fake tripping towards DSA is very important for the control center to improve network response against this kind of attack.

Traditionally, DSA includes multiple-algebra equations that could consume a long time to solve. Moreover, the study of DSA based on the normal contingencies that arises from lightning, normal failure of the protection devices, and overload. Recently, with the continued growth in the size of power networks, which is accompanied by implementation of many new technologies (e.g. as Phasor Measurement Units, smart grids and smart meters) that have helped to provide a snapshot for system state and at the same time leads to an increase in the data that needs to be processed when the contingency occurs. Additionally, with the increased probability of exposure to cyber-attacks on the power grid, the control center should develop a DSA tool that meets the needs for assessing dynamic security state with accurate result and a short time frame [9-12] and develop a better defense strategy to protect the power system against new threats that are fake tripping related and include it in simulations and analyses of the DSA tool.

In this study, a new approach has been developed for DSA tool to deal with online DSA challenges also to represent and analyze the effect of "fake tripping contingency" on the power system security via DSA tool. The target was to build an accurate and high-speed classifier. Thus the control center could trigger the accurate protection procedures to protect the power system where wrong protection steps could result in a high cost for the system operator.



## 1.2 Problem Statements

The power system network is one of the most complex human-made set-ups in the world. This network includes very large transmission line equipment that are installed in a sprawling geographical area which has different operation and environment factors. Security for power system is a crucial aspect, it prevents the occurrence of a blackout. Recently, the power system has witnessed many blackouts due to different types of contingencies affecting millions of people.

To ensure a continuous work of the power system network, control center must keep it in a secure state following contingencies to prevent blackout occurrence, DSA tool is used to evaluate the ability of the power system to withstand sudden disturbances and to survive the transition to an acceptable steady state. Then based

on the assessment for DSA, the operator could activate an accurate and fast protection processes to protect the network.

Based on the reviewed papers in this study, the new operating environment for power system made the DSA tool facing many challenges such as increased number of contingencies, a huge amount of measurement data stream from different network devices, which should be processed within a short time frame. Moreover, because the network is depending on the new weakly protected communication technology, a new threat to the power network which is originating from severe fake tripping contingency has appeared. This kind of contingency could be severe on the power security state due to the limitations of traditional defense and analysis strategies for the control center to deal with this kind of recent contingency.

There are several reported attempts to improve the DSA tools application in the literature such as the use of traditional time-domain simulation or data mining technologies. These approaches used the conventional DSA which is developed based on normal contingency evaluations only and this security criterion for power network operation is inadequate to address fake tripping contingency events. Despite the mentioned attempts, it remains a challenging task for the DSA tool in the present and future requirements to evaluate security system state due to the DSA computational complexity that is incurred by the massive scale data of the power network which increases every year and the large list of the contingencies.

Therefore, a new approach should be adopted to improve DSA classifier towards these recent and future challenges by trying to study the effect of a new threat of fake tripping contingency on power grid security state. Moreover, finding technical ways to reduce the stream dataset features in an effective way to enhance the result in terms of accuracy along with speed. The target is to build a robust DSA classifier that could be used to provide vital information for protection and control applications in power system operation to keep the network in a secure state and prevent the occurrence of blackouts.

Figure 1.2 briefly shows the research problem, its challenge, and the proposed solution.

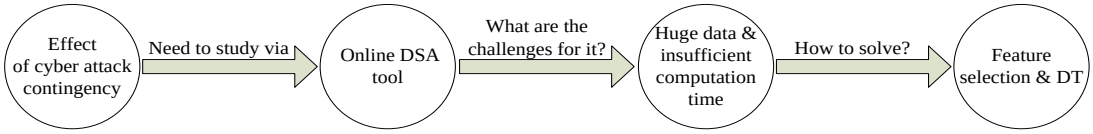


Figure 1.2: The main ideas of this study

## 1.3 Research Objectives

This research aims to achieve the following objectives:

i) To study the effects of fake tripping contingencies on the power system security via DSA.

ii) To develop a novel hybrid approach for DSA classifier based on advanced feature selection technique for decision tree (DT) classifier.

iii) To evaluate the performance of DSA classifier under normal and fake tripping contingencies, in terms of accuracy and computational time.

## 1.4 Research Scope

This research is limited to the following scope:

i) The simulators of the power system respond to normal and fake tripping contingencies for dynamic security assessment are carried out on the PowerWorld simulator platform.

ii) Symmetrical uncertainty (SU) is considered as a feature selection algorithm to reduce the redundant and irrelevant features in the dataset.

iii) Logistic Model Tree (LMT) is considered as the decision tree algorithm to develop the classifier model for the DSA.

iv) Waikato Environment for Knowledge Analysis (WEKA) program was uesd for implementing data mining technology.

v) The proposed algorithm is evaluated on the modified IEEE 9-bus, 14-bus, and 30-bus benchmark test systems model.

## REFERENCES


1. Sridhar, S., Hahn, A. and Govindarasu, M. Cyber-Physical System Security for the Electric Power Grid. *Proceedings of the IEEE*, 2012, 100(1): 210-224.
2. Xie, Z., Manimaran, G., Vittal, V., Phadke, A. G. and Centeno, V. An Information Architecture for Future Power Systems and its Reliability Analysis. *IEEE Transactions on Power Systems*, 2002, 17(3): 857-863.
3. Liscouski, B. and Elliot, W. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. *A Report to The US Department of Energy*, 2004 Apr, 40(4): 86.
4. Liang, G., Zhao, J., Luo, F., Weller, S. R. and Dong, Z. Y. A Review of False Data Injection Attacks Against Modern Power Systems. *IEEE Transactions on Smart Grid*, 2016, 8(4): 1630-1638.
5. Glenn, C., Sterbentz, D. and Wright, A. *Cyber Threat and Vulnerability Analysis of the US Electric Sector*. Idaho Falls, ID: Idaho National Lab. (INL). 2016.
6. Brinkhaus, S., Carluccio, D., Greveler, U., Justus, B., Löhr, D. and Wegener, C. Smart Hacking for Privacy. *Proceeding of the 28th Chaos Communication Congress (28C3)*, December 27-30. Berlin, Germany. 2011.
7. Zetter, K. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *Wired Magazine*, March 3, 2016.
8. Wang, Q., Tai, W., Tang, Y., Ni, M. and You, S. A Two-layer Game Theoretical Attack-defense Model for a False Data Injection Attack Against Power Systems. *International Journal of Electrical Power & Energy Systems*, 2019, 104: 169-177.
9. Alvarez, J. M. G. and Mercado, P. E. Online Inference of the Dynamic Security Level of Power Systems Using Fuzzy Techniques. *IEEE Transactions on Power Systems*, 2007, 22(2): 717-726.

10. Kerin, U., Heyde, C., Krebs, R. and Lerch, E. Real-time Dynamic Security Assessment of Power Grids. *The European Physical Journal Special Topics*, 223(12): 2503-2516.
11. Xue, Y., Yu, Y., Li, J., Gao, Z., Ding, C., Xue, F., Wang, L., Morison, G. K. and Kundur, P. A New Tool for Dynamic Security Assessment of Power Systems. *Control Engineering Practice*, 1998, 6(12): 1511-1516.
12. Geeganage, J., Annakkage, U. D., Weekes, T. and Archer, B. A. Application of Energy-Based Power System Features for Dynamic Security Assessment. *IEEE Transactions on Power Systems*, 2015, 30(4): 1957-1965.
13. Hemdan, N. G. and Kurrat, M. Efficient Integration of Distributed Generation for Meeting the Increased Load Demand. *International Journal of Electrical Power & Energy Systems*, 2011, 33(9): 1572-1583.
14. Liu, C., Sun, K., Rather, Z. H., Chen, Z., Bak, C. L., Thøgersen, P. and Lund, P. A Systematic Approach for Dynamic Security Assessment and the Corresponding Preventive Control Scheme Based on Decision Trees. *IEEE Transactions on Power Systems*, 2014, 29(2): 717-730.
15. El-Khattam, W., Abdelaziz, A. Y., Yahya, M. and El-Hadidy, M. Causes of the Blackout: The Grid Operation and Environment. *The 7th GCC CIGRE International Conference and the 16th Exhibition for Electrical Equipments*, November 22-24. Kuwait. 2011. 77-87.
16. Luo, F., Dong, Z., Chen, G., Xu, Y., Meng, K., Chen, Y. and Wong, K. Advanced Pattern Discovery-Based Fuzzy Classification Method for Power System Dynamic Security Assessment. *IEEE Transactions on Industrial Informatics*, 2015, 11(2): 416-426.
17. Alvarez, J. M. G., and Mercado, P. E. Online Inference of the Dynamic Security Level of Power Systems Using Fuzzy Techniques. *IEEE Transactions on Power Systems*, 2007, 22(2): 717-726.
18. Kundur, P., Paserba, J., Ajjarapu, V., Andersson, G., Bose, A., Canizares, C., Hatziargyriou, N., Hill, D., Stankovic, A., Taylor, C. and Van Cutsem, T. Definition and Classification of Power System Stability IEEE/CIGRE Joint Task Force on Stability Terms and Definitions. *IEEE Transactions on Power Systems*, 2004, 19(3): 1387-1401.
19. Zhang, Y., Wehenkel, L., Rousseaux, P. and Pavella, M. SIME: A Hybrid Approach to Fast Transient Stability Assessment and Contingency Selection.

*International Journal of Electrical Power & Energy Systems*, 1997, 19(3): 195-208.

20. Xu, Y., Dong, Z.Y., Zhao, J. H., Zhang, P. and Wong, K. P. A Reliable Intelligent System for Real-time Dynamic Security Assessment of Power System. *IEEE Transactions on Power Systems*, 2012, 27(3): 1253-1263.
21. Gu, C. and Jirutitijaroen, P. Dynamic State Estimation Under Communication Failure Using Kriging Based Bus Load Forecasting. *IEEE Transactions on Power Systems*, 2015, 30(6): 2831-2840.
22. Vaiman, M., Bell, K., Chen, Y., Chowdhury, B., Dobson, I., Hines, P., Papic, M., Miller, S. and Zhang, P. Risk Assessment of Cascading Outages: Methodologies and Challenges. *IEEE Transactions on Power Systems*, 2012, 27(2): 631-641.
23. Al-Gubri, Q. A., Ariff, M. and Saeh, I. Performance Analysis of Machine Learning Algorithms for Power System Dynamic Security Assessment. *4th IET Clean Energy and Technology Conference (CEAT 2016)*. November 14-15. Kuala Lumpur, Malaysia. 2016. 37-42.
24. Yang, Z., Jiang, X., Zhang, Z., Zhang, D. and Liu, Y. Study on the Influence Rules of Soluble Contaminants on Flashover Voltage of Disc Suspension Insulators. *IEEE Transactions on Dielectrics and Electrical Insulation*, 2016, 23(6): 3523-3530.
25. Morison, K. and Glavic, M. Review of On-Line Dynamic Security Assessment Tools and Techniques. CIGRE Working Group 601 of Study Committee C4 Final Report. January 2007.
26. Konstantinou, C. and Maniatakos, M. Impact of Firmware Modification Attacks on Power Systems Field Devices. *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, November 2-5. Miami, Florida. 2015.
27. Guajardo, L. T., Enríquez, A. C. and Leonowicz, Z. Error Compensation in Distance Relays Caused by Wind Power Plants in the Power Grid. *Electric Power Systems Research*, 2014, 106: 109-119.
28. Van Aalst, M. K. The Impacts of Climate Change on the Risk of Natural Disasters. *Disasters*, 2006, 30(1): 5-18.
29. Zhang, R., Xu, Y., Dong, Z. Y., Meng, K. and Xu, Z. Intelligent Systems for Power System Dynamic Security Assessment: Review and Classification. *4th*

*International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT)*, July 6-9. Weihai, Shandong, China. 2011. 134-139.

30. He, M., Vittal, V. and Zhang, J. Online Dynamic Security Assessment with Missing PMU Measurements: A Data Mining Approach. *IEEE Transactions on Power Systems*, 2013, 28(2): 1969-1977.
31. Sun, K., Likhate, S., Vittal, V., Kolluri, V. S. and Mandal, S. An Online Dynamic Security Assessment Scheme Using Phasor Measurements and Decision Trees. *IEEE Transactions on Power Systems*, 2007, 22(4): 1935-1943.
32. Meng, K., Dong, Z. Y., Wong, K. P., Xu, Y. and Luo, F. J. Speed-Up the Computing Efficiency of Power System Simulator for Engineering-Based Power System Transient Stability Simulations. *IET Generation, Transmission & Distribution*, 2010, 4(5): 652-661.
33. Tong, J. and Wang, L. Design of a DSA Tool for Real-Time Systems Operations. *International Conference on Power System Technology*, October 22-26. Chongqing, China. 2006. 1-5.
34. Schainker, R., Zhang, G., Hirsch, P. and Jing, C. Online Dynamic Stability Analysis Using Distributed Computing. *2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century*, July 20-24. Pittsburgh, Pennsylvania, USA. 2008. 1-7.
35. Smith, S., Woodward, C., Min, L., Jing, C., and Del Rosso, A. On-Line Transient Stability Analysis Using High-Performance Computing. *2014 IEEE PES Innovative Smart Grid Technologies Conference (ISGT),* February 19-22. Washington, DC. 2014. 1-5.
36. Huang, Z., Chen, Y. and Chavarría-Miranda, D. High-Performance Computing for Real-Time Grid Analysis and Operation. In: Khaitan, S. K. and Gupta, A. (Eds.). *High-Performance Computing in Power and Energy Systems.* Berlin, Heidelberg: Springer. 151-188; 2013.
37. Ashok, A., Govindarasu, M. and Wang, J. Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid. *Proceedings of the IEEE*, 2017, 105(7), 1389-1407.

38. Abdulrazzaq, A. A. Contingency Ranking of Power Systems Using a Performance Index. *International Research Journal of Engineering and Technology*, 2015, 2(2): 180-183.

39. Jmii, H., Meddeb, A., and Chebbi, S. (2018, March). Newton-Raphson Load Flow Method for Voltage Contingency Ranking. *2018 15th International Multi-Conference on Systems, Signals & Devices (SSD)*, March 19-22. Hammamet, Tunisia. 2018. 521-524.

40. Amjady, N. Dynamic Voltage Security Assessment by a Neural Network Based Method. *Electric Power Systems Research*, 2003, 66(3): 215-226.

41. Alvarez, J. M. G. Critical Contingencies Ranking for Dynamic Security Assessment Using Neural Networks. *15th International Conference on Intelligent System Applications to Power Systems*, November 8-12. Curitiba, Brazil. 2009. 1-6.

42. Ghosh, S. and Chowdhury, B. Design of An Artificial Neural Network for Fast Line Flow Contingency Ranking. *International Journal of Electrical Power & Energy Systems*, 1996, 18(5): 271-277.

43. Jain, T., Srivastava, L. and Singh, S. Fast Voltage Contingency Screening Using Radial Basis Function Neural Network. *IEEE Transactions on Power Systems*, 2003, 18(4): 1359-1366.

44. Swarup, K. S. Artificial Neural Network Using Pattern Recognition for Security Assessment and Analysis. *Neurocomputing*, 2008, 71(4): 983-998.

45. Xu, Y., Dong, Z. Y., Xu, Z., Meng, K. and Wong, K. P. An Intelligent Dynamic Security Assessment Framework for Power Systems with Wind Power. *IEEE Transactions on Industrial Informatics*, 2012, 8(4): 995-1003.

46. Morison, K. On-Line Dynamic Security Assessment Using Intelligent Systems. 2006 Power Engineering Society General Meeting, June 18-22. Montreal, Quebec, Canada. 2006. 1-5.

47. Zhang, D. and Li, S. Solving Optimal Dispatch Problem for a Competitive Wholesale Power Market by using PowerWorld. *2013 IEEE Power & Energy Society General Meeting*, July 21-25, Vancouver, Canada. 2013. 1-5.

48. Witten, I. H. and Frank, E. *Data Mining: Practical Machine Learning Tools and Techniques*. 2nd Edition. San Francisco, CA: Morgan Kaufmann Publishers. 2005.

49. Al-Masri, A. N., Ab Kadir, M. Z. A., Hizam, H. and Mariun, N. A Novel Implementation for generator Rotor Angle Stability Prediction Using An Adaptive Artificial Neural Network Application for Dynamic Security Assessment. *IEEE Transactions on Power Systems*, 2013, 28(3): 2516-2525.
50. Kucuktezcan, C. F. and Genc, V. I. A New Dynamic Security Enhancement Method via Genetic Algorithms Integrated with Neural Network-based Tools. *Electric Power Systems Research*, 2012, 83(1): 1-8.
51. Luo, F., Dong, Z., Chen, G., Xu, Y., Meng, K., Chen, Y. and Wong, K. Advanced Pattern Discovery-based Fuzzy Classification Method for Power System Dynamic Security Assessment. *IEEE Transactions on Industrial Informatics*, 2015, 11(2): 416-426.
52. Alvarez, J. M. G., and Mercado, P. E. A New Approach for Power System Online DSA Using Distributed Processing and Fuzzy Logic. Electric Power Systems Research, 2007, 77(2): 106-118.
53. He, M., Zhang, J. and Vittal, V. A Data Mining Framework for Online Dynamic Security Assessment: Decision Trees, Boosting, and Complexity Analysis. *3rd IEEE PES Conference on Innovative Smart Grid Technologies (ISGT 2012)*, January 16-20. Washington, DC. 2012. 1-8.
54. He, M., Zhang, J. and Vittal, V. Robust Online Dynamic Security Assessment Using Adaptive Ensemble Decision-Tree Learning. *IEEE Transactions on Power Systems*, 2013, 28(4), 4089-4098.
55. Liu, C., Sun, K., Rather, Z. H., Chen, Z., Bak, C. L., Thøgersen, P. and Lund, P. A Systematic Approach for Dynamic Security Assessment and the Corresponding Preventive Control Scheme Based on Decision Trees. *IEEE Transactions on Power Systems*, 2014, 29(2): 717-730.
56. Zhang, Y., Xu, Y., and Dong, Z. Y. Robust Ensemble Data Analytics for Incomplete PMU Measurements-Based Power System Stability Assessment. *IEEE Transactions on Power Systems*, 2018, 33(1): 1124-1126.
57. Dietterich, T. G. Ensemble Methods in Machine Learning. *International Workshop on Multiple Classifier Systems*, June 21-23. Cagliari, Italy. 2000. 1-15.
58. Hall, M. A. *Correlation-based Feature Selection for Machine Learning*. Ph.D. Thesis, University of Waikato. 1999.

59. Morris, T. H., Pan, S., Adhikari, U., Younan, N., King, R. and Madani, V. Phasor Measurement Unit and Phasor Data Concentrator Cyber Security. In: Pappu, V., Carvalho, M. and Pardalos, P. (Eds.). *Optimization and Security Challenges in Smart Power Grids*. Berlin, Heidelberg: Springer. 141-159; 2013.

60. Ariff, M. A. M., Pal, B. C. and Singh, A. K. Estimating Dynamic Model Parameters for Adaptive Protection and Control in Power System. *IEEE Transactions on Power Systems*, 2015, 30(2): 829-839.

61. Adhikari, U., Morris, T. H., Dahal, N., Pan, S., King, R. L., Younan, N. H. and Madani, V. Development of Power System Test Bed for Data Mining of Synchrophasors Data, Cyber-Attack and Relay Testing in RTDS. *2012 IEEE Power & Energy Society General Meeting*, July 22-26. San Diego, California. 2012. 1-7.

62. Hink, R. C. B., Beaver, J. M., Buckner, M. A., Morris, T., Adhikari, U. and Pan, S. Machine Learning for Power System Disturbance and Cyber-Attack Discrimination. *2014 7th International Symposium on Resilient Control Systems (ISRCS 2014)*, August 19-21. Denver, Colorado. 2014. 1-8.

63. Narendra, K. and Weekes, T. Phasor Measurement Unit (PMU) Communication Experience in a Utility Environment. *Conference on Power Systems*, October 19-21. Winnipeg, Canada. 2008.

64. Khan, S. H., Imtiaz, S., Mustafa, H., Aijaz, A. and Ali, M. Design and Development of a Synchrophasor Measurements Unit as per IEEE Standard C37. 118.1-2011. 2014.

65. Jia, Y., Xu, Z., Lai, L. L. and Wong, K. P. Risk-Based Power System Security Analysis Considering Cascading Outages. *IEEE Transactions on Industrial Informatics*, 2016, 12(2): 872-882.

66. Pan, S., Morris, T. and Adhikari, U. Classification of Disturbances and Cyber-Attacks in Power Systems Using Heterogeneous Time-Synchronized Data. *IEEE Transactions on Industrial Informatics*, 2015, 11(3): 650-662.

67. Wang, J., Hui, L. C., Yiu, S. M., Wang, E. K. and Fang, J. A Survey on Cyber Attacks Against Nonlinear State Estimation in Power Systems of Ubiquitous Cities. *Pervasive and Mobile Computing*, 2017, 39: 52-64.

68. Bretas, A. S., Bretas, N. G., Carvalho, B., Baeyens, E. and Khargonekar, P. P. Smart Grids Cyber-Physical Security as a Malicious Data Attack: An Innovation Approach. *Electric Power Systems Research*, 2017, 149: 210-219.

69. Ghanem, W. A. H., and Belaton, B. (2013, November). Improving Accuracy of Applications Fingerprinting on Local Networks Using NMAP-AMAP-ETTERCAP as a Hybrid Framework. *2013 IEEE International Conference on Control System, Computing and Engineering (ICCSCE)*, November 29 – December 1. Parkroyal Penang Resort, Batu Ferringhi, Penang, Malaysia. 2013. 403-407.

70. Morris, T. H., Pan, S., and Adhikari, U. (2012, July). Cyber Security Recommendations for Wide Area Monitoring, Protection, and Control Systems. *2012 IEEE Power & Energy Society General Meeting*, July 22-26. San Diego, California. 2012. 1-6.

71. Rahman, A., and Ali, M. Analysis and Evaluation of Wireless Networks by Implementation of Test Security Keys. *International Conference for Emerging Technologies in Computing*, August 23-24. London, UK. 2018. 107-126.

72. Hink, R. C. B., Beaver, J. M., Buckner, M. A., Morris, T., Adhikari, U., and Pan, S. Machine Learning for Power System Disturbance and Cyber-Attack Discrimination. *2014 7th International Symposium on Resilient Control Systems (ISRCS)*, August 19-21. Denver, Colorado. 2014. 1-8.

73. Pan, S., Morris, T., and Adhikari, U. Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems. *IEEE Transactions on Smart Grid*, 2015, 6(6): 3104-3113.

74. Morison, K., Wang, L., and Kundur, P. Power System Security Assessment. *IEEE Power and Energy Magazine*, 2004, 2(5): 30-39.

75. Al-Gburi, Q. A., and Ariff, M. A. M. Dynamic Security Assessment for Power System Under Cyber-Attack. *Journal of Electrical Engineering & Technology*, 2019: 1-11.

76. Pasqualetti, F., Dörfler, F., and Bullo, F. Attack Detection and Identification in Cyber-Physical Systems. *IEEE Transactions on Automatic Control*, 2013, 58(11): 2715-2729.

77. Pan, S., Morris, T. and Adhikari, U. Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems. *IEEE Transactions on Smart Grid*, 2015, 6(6): 3104-3113.

78. Chen, Y., Hong, J. and Liu, C. C. Modeling of Intrusion and Defense for Assessment of Cyber Security at Power Substations. *IEEE Transactions on Smart Grid*, 2016.

79. Adhikari, U., Morris, T. H., and Pan, S. Applying Non-Nested Generalized Exemplars Classification for Cyber-Power Event and Intrusion Detection. *IEEE Transactions on Smart Grid*, 2016.

80. Adhikari, U., Morris, T. and Pan, S. Applying Hoeffding Adaptive Trees for Real-Time Cyber-Power Event and Intrusion Classification. *IEEE Transactions on Smart Grid*, 2017.

81. Sridhar, S., Govindarasu, M., and Liu, C. C. (2012). Risk analysis of coordinated cyber attacks on power grid. In: Chakrabortty, A., & Ilić, M. D. (Eds.). *Control and Optimization Methods for Electric Smart Grids* (Vol. 3). New York, NY: Springer Science & Business Media. 275-294; 2012.

82. Cleveland, F. M. Cyber Security Issues for Advanced Metering Infrastructure (AMI). *IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, July 20-24. Pittsburgh, PA. 2008. 1-5.

83. Wang, W. and Lu, Z. Cyber Security in the Smart Grid: Survey and Challenges. *Computer Networks*, 2013, 57(5): 1344-1371.

84. Pappu, V., Carvalho, M. and Pardalos, P. (Eds.). *Optimization and Security Challenges in Smart Power Grids.* New York: Springer. 2013.

85. Liu, S., Liu, X .P. and El Saddik, A. Denial-of-Service (DoS) Attacks on Load Frequency Control in Smart Grids. *2013 IEEE PES Innovative Smart Grid Technologies (ISGT)*, February 24-27. Washington, DC. 2013. 1-6.

86. Rasmussen, T. B., Yang, G., Nielsen, A. H. and Dong, Z. A Review of Cyber-Physical Energy System Security Assessment. *2017 IEEE PES PowerTech Conference (PowerTech 2017)*, June 18-22. Manchester, UK. 2017.

87. Pillitteri, V. Y. and Brewer, T. L. *Guidelines for Smart Grid Cybersecurity*. NIST Interagency/Internal Report (NISTIR)-7628 Rev 1. 2014.

88. Hahn, A., Ashok, A., Sridhar, S., and Govindarasu, M. Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid. *IEEE Transactions on Smart Grid*, 2013, 4(2): 847-855.

89. Xiang, Y., Ding, Z., Zhang, Y. and Wang, L. Power System Reliability Evaluation Considering Load Redistribution Attacks. *IEEE Transactions on Smart Grid*, 2017, 8(2): 889-901.

90. Romeis, C. and Jaeger, J. Dynamic Protection Security Assessment, A Technique for Blackout Prevention. *2013 IEEE Grenoble Conference PowerTech*, June 16-20. Grenoble, France. 2013. 1-6.

91. Cutsem, T. V., Ribbens-Pavella, M., and Mili, L. Bad Data Identification Methods in Power System State Estimation-A Comparative Study. *IEEE Transactions on Power Apparatus and Systems*, 1985, PAS-104(11): 3037-3049.

92. Monticelli, A., and Garcia, A. Reliable Bad Data Processing for Real-Time State Estimation. *IEEE Transactions on Power Apparatus and Systems*, 1983, PAS-102(5): 1126-1139.

93. Nian-De, X., Shi-Ying, W., and Er-Keng, Y. A New Approach for Detection and Identification of Multiple Bad Data in power System State Estimation. *IEEE Transactions on Power Apparatus and Systems*, 1982, PAS-101(2): 454-462.

94. Quintana, V. H., Simoes-Costa, A., and Mier, M. Bad Data Detection and Identification Techniques Using Estimation Orthogonal Methods. *IEEE Transactions on Power Apparatus and Systems*, 1982, PAS-101(9), 3356-3364.

95. Xu, R., Wang, R., Guan, Z., Wu, L., Wu, J., and Du, X. Achieving Efficient Detection Against False Data Injection Attacks in Smart Grid. *IEEE Access*, 2017, 5, 13787-13798.

96. Bobba, R. B., Rogers, K. M., Wang, Q., Khurana, H., Nahrstedt, K., and Overbye, T. J. Detecting False Data Injection Attacks on DC State Estimation. *Preprints of the First Workshop on Secure Control Systems, CPSWEEK* 2010, April 12. Stockholm, Sweden. 2010.

97. Zhuang, P., Deng, R., and Liang, H. False Data Injection Attacks Against State Estimation in Multiphase and Unbalanced Smart Distribution Systems. *IEEE Transactions on Smart Grid*, 2019, 1(1).

98. Kundur, P., Balu, N. J., and Lauby, M. G. (1994). *Power System Stability and Control* (Vol. 7). New York: McGraw-Hill.

99. Zhang, Y., Wehenkel, L., Rousseaux, P., and Pavella, M. SIME: A Hybrid Approach to Fast Transient Stability Assessment and Contingency Selection. *International Journal of Electrical Power & Energy Systems*, 1997, 19(3): 195-208.

100. Vu, T. L., and Turitsyn, K. Lyapunov Functions Family Approach to Transient Stability Assessment. *IEEE Transactions on Power Systems*, 2016, 31(2): 1269-1277.

101. Xue, Y., Yu, Y., Li, J., Gao, Z., Ding, C., Xue, F., Wang, L., Morison, G. K., and Kundur, P. (1998). A New Tool for Dynamic Security Assessment of Power Systems. *Control Engineering Practice*, 1998, 6(12): 1511-1516.

102. McCalley, J. D., Wang, S., Zhao, Q. L., Zhou, G. Z., Treinen, R. T., & Papalexopoulos, A. D. Security Boundary Visualization for Systems Operation. IEEE Transactions on Power Systems, 1997, 12(2), 940-947.

103. Savulescu, S. C. *Real-time Stability Assessment in Modern Power System Control Centers* (Vol. 42). John Wiley & Sons. 2009.

104. Vittal, V., Sauer, P., Meliopoulos, S., and Stefopoulos, G. K. On-line Transient Stability Assessment Scoping Study. Final Project Report, PSERC Publication, 2005, 05-04.

105. Xu, Y., Dong, Z. Y., Zhao, J. H., Zhang, P., and Wong, K. P. A Reliable Intelligent System for Real-Time Dynamic Security Assessment of Power Systems. *IEEE Transactions on Power Systems*, 2012, 27(3): 1253-1263.

106. Luo, F., Dong, Z., Chen, G., Xu, Y., Meng, K., Chen, Y., & Wong, K. (2015). Advanced Pattern Discovery-Based Fuzzy Classification Method for Power System Dynamic Security Assessment. *IEEE Transactions on Industrial Informatics*, 2015, 11(2): 416-426.

107. Witten, I. H., Frank, E., Hall, M. A., and Pal, C. J. *Data Mining: Practical Machine Learning Tools and Techniques*. 4th Edition. San Francisco, CA: Morgan Kaufmann Publishers. 2016.

108. Yu, L. and Liu, H. Feature Selection for High-Dimensional Data: A Fast Correlation-Based Filter Solution. *Proceedings of the 20th International Conference on Machine Learning* (pp. 856-863), Menlo Park, CA: The AAAI Press. 2003.

109. Kannan, S. S., and Ramaraj, N. A Novel Hybrid Feature Selection via Symmetrical Uncertainty Ranking Based Local Memetic Search Algorithm. *Knowledge-Based Syst*em, 2010; 23: 580-585.

110. Yu, L. and Liu, H. Efficient Feature Selection via Analysis of Relevance and Redundancy. *Journal of Machine Learning Research*, 2004; 5: 1205-1224.

111. Kaladhar, D. S., Chandana, B. and Kumar, P. B. Predicting Cancer Survivability Using Classification Algorithms. *LMT*, 2011, 34(65.7): 96-106.

112. Ruiz, R., Riquelme, J. C. and Aguilar-Ruiz, J. S. Incremental Wrapper-Based Gene Selection from Microarray Data for Cancer Classification. *Pattern Recognition*, 2006, 39(12): 2383-2392.

113. Kumar, A. and Zhang, D. Personal Recognition Using Hand Shape and Texture. *IEEE Transactions on Image Processing*, 2006, 15(8): 2454-2461.

114. Landwehr, N., Hall, M. and Frank, E. Logistic Model Trees. *Machine Learning*, 2005, 59(1-2): 161-205.

115. Demetriou, P., Asprou, M., Quiros-Tortos, J. and Kyriakides, E. Dynamic IEEE Test Systems for Transient Analysis. *IEEE Systems Journal*. 2015.

116. Hutcheon, N. and Bialek, J. W. Updated and Validated Power Flow Model of the Main Continental European Transmission Network. *2013 IEEE Grenoble Conference PowerTech*, June 16-20. Grenoble, France. 2013. 1-5.

117. PowerWorld Corporation. *Simulator*: *PowerWorld Simulator*. Retrieved from https://www.powerworld.com/products/simulator/overview.

118. Chen, Jingnian, Houkuan Huang, Fengzhan Tian, and Shengfeng Tian. A Selective Bayes Classifier for Classifying Incomplete Data Based on Gain Ratio. Knowledge-Based Systems 21, 2008, 7: 530-534.

119. Günal, Serkan. Hybrid Feature Selection for Text Classification. Turkish Journal of Electrical Engineering & Computer Sciences 20, 2012, Sup. 2: 1296-1311.

120. Huang, Yue, Paul J. McCullagh, and Norman D. Black. An Optimization of Relief for Classification in Large Datasets. Data & Knowledge Engineering 68, 2009, 11: 1348-1356H

121. Elomaa, Tapio, and Matti Kaariainen. An Analysis of Reduced Error Pruning. *Journal of Artificial Intelligence Research*, 2001: 163-187.

122. Yadav, Amit Kumar, and S. S. Chandel. Solar Energy Potential Assessment of Western Himalayan Indian State of Himachal Pradesh Using J48

Algorithm of WEKA in ANN Based Prediction Model. *Renewable Energy*, 2015: 675-693.

123. Sahu, S., & Mehtre, B. M. Network Intrusion Detection System using J48 Decision Tree. *IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. 2015. 2023-2026.

124. Yan, Ye, Yi Qian, Hamid Sharif, and David Tipper. A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. *IEEE Communications Surveys & Tutorials*, 2013, 15(1): 5-20.

125. Kundur, P., C. Taylor, and P. Pourbeik. Blackout Experiences and Lessons, Best Practices for System Dynamic Performance, and the Role of New Technologies. *IEEE Task Force Report*. 2007.